CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Análise de Sistemas e Tecnologia da Informação: Segurança da Informação

Mateus Castilho Reversi

CONTINUIDADE DOS SERVIÇOS DE TI

Americana, SP

2015

CENTRO PAULA SOUZA

FACULDADE DE TECNOLOGIA DE AMERICANA

Análise de Sistemas e Tecnologia da Informação: Segurança da Informação

Mateus Castilho Reversi

CONTINUIDADE DOS SERVIÇOS DE TI

Trabalho de Conclusão de Curso desenvolvido em cumprimento à exigência curricular do Curso Segurança da Informação, sob a orientação do Prof. Especialista Edson Roberto Gaseta.

Área de concentração: Segurança da Informação.

Americana, S. P.

2015

Dados Internacionais de Catalogação-na-fonte

R349c

Reversi, Mateus Castilho

Continuidade dos serviços de TI. / Mateus Castilho Reversi. – Americana: 2015.

39f.

Monografia (Graduação em Tecnologia em Segurança da Informação). - - Faculdade de Tecnologia de Americana – Centro Estadual de Educação Tecnológica Paula Souza.

Orientador: Prof. Esp. Edson Roberto Gaseta

1. Sistemas de informação I. Gaseta, Edson Roberto II. Centro Estadual de Educação Tecnológica Paula Souza – Faculdade de Tecnologia de Americana.

CDU: 681.518

Mateus Castilho Reversi

CONTINUIDADE DOS SERVIÇOS DE TI

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em Segurança da Informação pelo CEETEPS/Faculdade de Tecnologia – Fatec/ Americana.
Área de concentração: Segurança da Informação.

Americana, 07 de dezembro de 2015.

Banca Examinadora:

Edson Roberto Gaseta (Presidente)
Especialista
FATEC Americana

Benedito Aparecido Cruz (Membro)
Graduado
FATEC Americana

Adnan Bakri (Membro)
Especialista
FATEC Americana

AGRADECIMENTOS

Agradeço a Deus pela minha família que me apoia em todos os aspectos da minha vida. Rose, Daniela, Luiza, Zilda e Antônio, com vocês foi mais fácil chegar até aqui e sou grato todos os dias. À minha namorada Fernanda, pelo seu companheirismo e presença constante em minha vida.

DEDICATÓRIA

À memória de meu pai Luiz, que sempre me incentivou e certamente estaria muito orgulhoso.

RESUMO

O presente trabalho conceitua disponibilidade de serviços de TI e sua importância para manter vivo o negócio de uma organização. A garantia dessa disponibilidade é um dos pilares essenciais da segurança da informação. Como requisito da segurança da informação é necessário entender os riscos atrelados e os impactos que uma indisponibilidade de serviços pode causar à organização. Para assegurar a alta disponibilidade dos serviços de TI, cada empresa deve apresentar um plano de continuidade. Os planos de continuidade devem ser avaliados periodicamente para determinar que sejam maduros, estruturados, testados e continuamente aferidos, garantindo assim sua eficiência. No estudo de caso apresentado, foi elaborado um questionário para avaliar o nível de maturidade do processo utilizado para assegurar a disponibilidade de serviços de TI de uma determinada empresa do setor financeiro. O questionário foi baseado no processo DS4 das boas práticas do COBIT 4.1. As respostas obtidas foram analisadas, utilizando-se o COBIT como mecanismo de avaliação do processo. Foi identificado que a empresa se encontra num nível aceitável de maturidade estabelecida pelo mercado, requerendo poucas melhorias para alcançar um nível maior de sua maturidade. Por fim, foram feitas algumas recomendações baseadas no modelo COBIT, padrão internacionalmente reconhecido.

Palavras Chave: Continuidade de negócios; Nível de maturidade; COBIT.

ABSTRACT

The present work conceptualizes IT service availability and its importance to keep alive the business of an organization. The guarantee of this availability is one of the essential pillars of security information. As a security information requirement it is necessary to understand the risks and impacts that an unavailability of services can cause to the organization. To ensure high availability of IT services, each company must have a continuity plan. The continuity plans should be evaluated periodically to determine if they are mature, structured, tested and continuously measured, thereby ensuring their efficiency. In the present case study, a questionnaire was designed to evaluate the process maturity level used to ensure the IT availability services of a financial company. The questionnaire was based on the DS4 process of COBIT 4.1 best practices. The given responses were analyzed using COBIT as an evaluation mechanism of the process. It was identified that the company is at an acceptable level established by the market maturity, requiring few improvements to achieve a higher level of maturity. At last, some recommendations were made based on the COBIT model, internationally recognized standard.

Keywords: *Maturity level; Business Continuity; COBIT.*

SUMÁRIO

LISTA DE FIGURAS E DE TABELAS

1 INTRODUÇÃO

Atualmente, o mundo está altamente conectado, onde todos esperam que os serviços de tecnologia respondam imediatamente, o que requer sistemas de informação entregando dados com alta disponibilidade. É grande a dependência das organizações no que diz respeito à Tecnologia da Informação (TI), sejam as organizações de pequeno, médio ou grande porte. Caso alguma interrupção ocorra, é esperado que os serviços se reestabeleçam de forma rápida e com sua capacidade anterior, e, na medida do possível, com transparência ao consumidor.

O objetivo geral foi discutir os processos, alguns métodos e soluções para a continuidade de serviços de TI.

Como objetivos específicos ficou estabelecido o foco na avaliação da continuidade de serviços de TI, baseado no modelo COBIT 4.1, e seu respectivo processo DS4 - Assegurar a Continuidade dos Serviços.

O método científico de pesquisa utilizado foi a avaliação do processo do COBIT 4.1, baseado no seu nível de maturidade, utilizando os controles para a avaliação.

O trabalho foi estruturado em cinco capítulos, sendo que o primeiro apresenta conceitos de Segurança da Informação e os fatores que garantem a disponibilidade de serviço, o segundo capítulo aborda a continuidade de serviços de TI e o plano de continuidade de negócios. O terceiro capítulo discute questões relacionadas à maturidade do processo.

O quarto capítulo apresenta-se a metodologia utilizada para a avaliação de um processo fazendo-se o uso das boas práticas do modelo COBIT e os resultados alcançados. No quinto capítulo encontra-se as considerações finais.

2 SEGURANÇA DA INFORMAÇÃO

A informação é um recurso crítico para as organizações, que dependem cada vez mais da informação para a estabilidade de seus serviços, de modo a se manter competitiva e atingir o seu principal objetivo, o sucesso de seu negócio. Sendo assim, pode-se classificar a informação como um dos ativos mais importantes dentro da organização. Dada tamanha importância da informação é necessário garantir sua proteção através de políticas e regras. Cabe ao setor de segurança da informação definir regras a serem seguidas por todos funcionários, através de políticas de segurança, independentemente do tipo de negócio ou porte da organização.

É considerado seguro o negócio que atender aos três pilares básicos que mantém e norteiam a segurança da informação: confidencialidade, integridade e disponibilidade. A seguir, Lyra (2008) e Sêmola (2002) apresentam as características de cada um deles e o que eles garantem:

Confidencialidade: é o pilar que visa garantir que toda informação seja protegida de acordo com a sua classificação e que o acesso seja restrito apenas às pessoas devidas. Para isso pode-se usar recursos como senhas ou criptografia dos dados.

Integridade: é o pilar que visa prevenir que a informação seja alterada, garantindo que ela permaneça da forma como foi disponibilizada.

Disponibilidade: é o pilar que trata da garantia de acesso à informação. Apoiado nos pilares anteriores, a disponibilidade é o fator chave e de maior interesse nesse trabalho. É fundamental que cada usuário tenha livre acesso às informações que lhe sejam pertinentes a qualquer momento que seja necessário ou conveniente. Sem a disponibilidade, os demais pilares perdem sua significância.

Sendo assim, a disponibilidade significa que a informação deve estar pronta para quando necessário seu uso. Garantir que isso de fato ocorra, porém, exige que os ativos que suportam a informação estejam sempre disponíveis, tornando este pilar de grande complexidade para sua efetivação.

2.1 DISPONIBILIDADE

De acordo com Brown e Stallings (2014), o nível de disponibilidade vai depender de quão crítico é o serviço de TI, quanto mais alta sua criticidade, maior é o nível de disponibilidade. Complementam:

> "[...]. Considere um sistema que provê serviços de autenticação para sistemas, aplicações e dispositivos críticos. Uma interrupção do serviço resultaria na incapacidade de os clientes acessarem ativos computacionais e de funcionários acessarem os ativos de que necessitam para executar tarefas críticas. A perda do serviço traduz-se em grande perda financeira e em termos de perda de produtividade dos empregados e potencial perda de clientes ".

Para Magalhães e Pinheiro (2007), disponibilidade pode ser compreendida como o percentual que um serviço de TI esteja disponível para uso. Mas como aumentar a disponibilidade de um serviço? Isso pode ser feito através de mecanismos de detecção e recuperação de falhas. Todo negócio que demanda alto percentual de serviço disponível, é considerado de alta disponibilidade.

A alta disponibilidade é um dos conceitos mais preciosos dentro da área de tecnologia da informação. Massiglia e Marcus (2002), apontam que para as organizações que possuem serviços vitais para seus negócios, apenas manter estes serviços disponíveis não é suficiente, eles desejam que estes dados estejam altamente disponíveis, em outras palavras, vale um investimento para ter uma redundância de equipamentos de TI que possam manter o funcionamento contínuo dos serviços. Com a grande dependência das organizações no ambiente de TI, justificam altos investimentos em alta disponibilidade.

Assim como acontece em nosso dia a dia, onde espera-se que ao ligar a chave de um veículo o mesmo venha a funcionar de imediato, o mesmo é esperado em um ambiente de tecnologia, todos esperam ter seu serviço disponível a qualquer momento, exceto quando o serviço entra em rotinas de manutenção, que devem ser previamente e claramente comunicadas aos usuários.

O sucesso de uma organização está devidamente atrelado à qualidade de entrega dos serviços que, por sua vez, dependem da disponibilidade dos recursos necessários para manter o ambiente tecnológico. Por isso, surgem algumas preocupações básicas como riscos e incidentes.

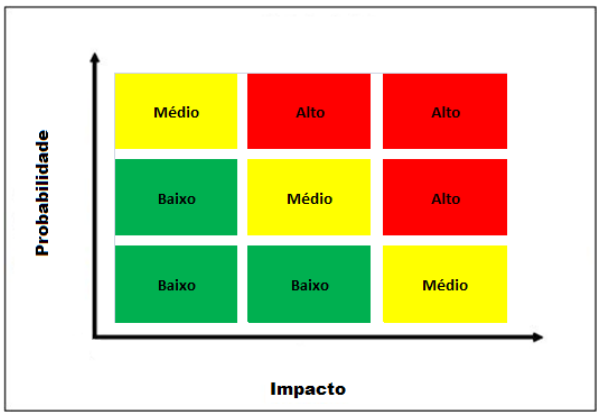
Para isso é fundamental que a organização entenda os riscos que possam afetar a disponibilidade de serviços, isto pode ser feito através da gestão de riscos, assunto discutido no próximo capítulo.

2.2 GESTÃO DE RISCOS, INCIDENTE E IMPACTO:

Ferreira e Araújo (2008) definem a gestão de riscos como um programa que faz parte da política de segurança, que tem por finalidade monitorar e tratar os riscos do ambiente tecnológico. No entanto COBIT (2007) apresenta a gestão de riscos como uma preocupação a ser tratada por especialistas da corporação deixando explícito que se trata de um item indispensável nas atividades da organização.

Risco é uma condição incerta, que, se ocorrer pode gerar um efeito positivo ou negativo para a companhia. Alevate (2014) diz que risco está associado a probabilidade de um incidente ocorrer através de vulnerabilidades. A relação entre risco e criticidade fazem parte da continuidade de negócios, e através da junção de impacto e probabilidade que é determinado a prioridade de um incidente, conhecida como matriz de risco. A Figura 1 mostra uma matriz de risco.

Figura 1 - Matriz de risco



Fonte: Adaptado de Magalhães e Pinheiro (2007).

Sendo assim, pode-se afirmar que risco se trata de condição duvidosa, o que leva as organizações a tratarem o risco como algo negativo considerando o que pode ocorrer de pior para seus negócios. O plano de continuidade visa a redução de vulnerabilidade e impacto, mesmo sabendo que riscos estarão sempre presentes, o

ideal é mensurar os riscos levando em conta as possíveis vulnerabilidades e suas consequências, os impactos.

O modelo COBIT (2007) aponta que os riscos relacionados a TI estão cada vez mais complexos, sendo necessário um bom gerenciamento dos riscos encontrados a fim de reduzir o efeito sobre os negócios da organização.

A avaliação de riscos é um processo que identifica todos os recursos críticos da organização e as ameaças que podem afetar estes recursos. Lyra (2008) diz que este processo pode definir prováveis cenários que possam vir afetar a organização com interrupções ou até mesmo desastres. Através da etapa de avaliação de riscos, a área de TI determina os possíveis danos a cada serviço e define medidas de prevenção, visando reduzir os efeitos de perda. O autor reforça que esta atividade envolve o centro de custos da organização, uma vez que com o retorno da avaliação de riscos, é possível que tenha a necessidade de corrigir ou até mesmo implementar uma nova solução no ambiente tecnológico.

De acordo com a ITIL (*Information Technology Infrastructure Library*), incidente pode ser um evento que não faz parte da operação normal de um determinado serviço. Lyra (2008) diz que:

> “[...]. Um incidente de segurança é a ocorrência de um evento que possa causar interrupções nos processos de negócio em consequência da violação de algum dos aspectos listados acima”.

Um incidente pode ocasionar um impacto nos serviços da organização, que pode estar associado a um risco que foi ou não avaliado pelo processo de avaliação de risco.

A melhor maneira de estudar os impactos de uma organização é através da análise de impacto nos negócios, que está presente no plano de continuidade de negócios.

No próximo capítulo será discutido uma vertente da segurança da informação, a continuidade de serviços de TI.

3 CONTINUIDADE DE SERVIÇOS DE TI

A definição de serviço em TI, de acordo com Abreu e Fernandes (2014) apontam que:

> “[...]. De acordo com a ITIL, um serviço é um "meio de entregar valor aos clientes, facilitando o atingimento dos resultados que os clientes desejam, tirando deles a propriedade dos custos e riscos específicos". Pela perspectiva do cliente, a criação do valor de um serviço é uma função de duas variáveis: a utilidade (possui o desempenho desejado ou redução das restrições de desempenho) e a garantia (disponibilidade, capacidade, continuidade e segurança suficientes para o uso) ”.

Com base no que o autor cita acima, serviço é qualquer recurso que se torna valioso para a organização e sua indisponibilidade acarreta em um resultado inesperado ou indesejado.

No ponto de vista de Magalhães e Pinheiro (2007):

> “[...]. A continuidade dos serviços de TI pode ser definida como um suporte de processos de negócio que visam garantir que os serviços possam ser recuperados de forma rápida. Para tal faz-se necessário ter um Plano de continuidade de negócio.
>
> O plano de continuidade de serviços é um conjunto de medidas estratégicas definidas por uma equipe responsável, nomeada pela alta gerência da organização. Cabe a eles definirem procedimentos necessários com ações preventivas e de continuidade da normalidade dos serviços de informação, de forma a preparar a organização ou uma área especifica desta organização, na provável ocorrência de uma indisponibilidade de informações”.

Recomenda-se que a equipe citada pelo autor ou parte dela, tenha participado da elaboração do plano de continuidade de negócios da empresa.

Este plano de continuidade de serviços da empresa passa por diversas etapas e uma delas é a análise de vulnerabilidades e de riscos dos ativos da organização, elaborando um relatório que prioriza as vulnerabilidades e os riscos.

De acordo com Massiglia e Marcus (2002), os riscos mais comuns na ocorrência de uma indisponibilidade são: falhas humanas, tecnológicas e causas naturais.

Para manter a alta disponibilidade é necessário antecipar as falhas mais comuns, mantendo sempre os dispositivos físicos (*hardware*) e os sistemas (*software*)

monitorados e ter procedimentos para quando um dos componentes falhar, a recuperação seja rápida e imperceptível.

Magalhães e Pinheiro (2007, p.72) reforçam que o plano de continuidade de serviço não deve ser reativo, porém deve contemplar medidas proativas na mitigação dos riscos encontrados em consequência de uma indisponibilidade.

No capítulo a seguir, será mostrado o plano de continuidade de negócio, que segundo os mesmos autores, é “desenvolvido não apenas para garantir a recuperação e a disponibilização dos serviços de TI, mas também com uma visão de recuperação do processo de negócio”.

3.1 PLANO DE CONTINUIDADE DE NEGÓCIOS

O tema continuidade de negócios é vasto e abrangente. Um Plano de Continuidade de Negócios deve seguir normas claras, definidas e detalhadas.

Neste contexto, Magalhães e Pinheiro (2007) dizem que:

> "[...] o objetivo do PCN é traçar uma estratégia, com todos os procedimentos necessários, no sentido de garantir o restabelecimento dos sistemas corporativos, no menor espaço de tempo possível. Ou seja, é um conjunto de diretrizes que permitem recuperar a operação com agilidade, priorizando os sistemas críticos da corporação. "

O PCN (Plano de Continuidade de Negócios) dentro de uma organização visa manter o funcionamento de seus ativos, caso um desastre ocorra.

Os ativos de uma empresa são considerados elementos de valor para a organização e por isso requerem medidas de segurança que garantam a proteção dos mesmos.

Fontes (2006) cita: "Toda organização deve estar preparada para enfrentar situações de contingência e de desastre que tornem indisponíveis recursos que possibilitam seu uso. "

Com base neste contexto, o mesmo autor complementa "Toda informação deve ser protegida contra desastres físicos (fogo, calor, inundação etc.) e lógicos (vírus, acesso indevido, erro de programas, alteração incorreta etc.) ".

Alevate (2014, p.6.) faz uma analogia utilizando seguros de carros para representar a continuidade de negócios, ele diz que as seguradoras fornecem um veículo extra durante o conserto do avariado, o período que este ficará sob a responsabilidade do cliente depende do tamanho do investimento, caso este não tenha como arcar com o plano oferecido pela seguradora, ficará sem carro, e, por consequência, sem continuidade. O autor ainda complementa:

> "[...]. Enfim, diversas são as alternativas (contingências), mas qualquer delas só terá sucesso se analisadas antes da ocorrência do problema. Isto é continuidade".

Porém antes de começar com um plano de continuidade de negócios, a organização precisa passar por uma avaliação de risco e análise de impacto nos negócios. Sobre este assunto, Fontes (2008) apresenta alguns pontos a serem

considerados pela organização durante a preparação do plano de continuidade de negócio:

Avaliação de ameaças e riscos: este é o primeiro passo a ser tomado pela organização após definido os ativos e prioridades. Com esta análise deve-se determinar o potencial de um risco associado aos serviços disponibilizados. Lyra (2008) diz que o processo relacionado à avaliação e controle de riscos devem definir possíveis e prováveis cenários que possam afetar a organização, riscos que fazem parte do cotidiano do mundo corporativo e que podem afetar a organização tanto com interrupções quanto desastres.

Análise de impacto no negócio: Sêmola (2002) descreve de forma clara o que é a análise de impacto no negócio:

> "[...]. Conhecido mundialmente pela sigla BIA - *Business Impact Analysis*, esta primeira etapa é fundamental por fornecer informações para o perfeito dimensionamento das demais fases de construção do plano de continuidade. Seu objetivo é levantar o grau de relevância entre os processos ou atividades que fazem parte do escopo da contingência em função da continuidade do negócio. Em seguida, são mapeados os ativos físicos, tecnológicos e humanos que suportam cada um deles, para então apurar os impactos quantitativos que poderiam ser gerados com a sua paralisação total ou parcial".

Para Lyra (2008), esta etapa identifica e avalia os impactos que possam afetar a organização, como interrupção ou desastre. O processo de análise utiliza técnicas que definem a criticidade e prioridades de recuperação dos recursos do negócio, ela também quantifica e qualifica os impactos, sempre atentando aos prazos estabelecidos pela direção.

Elaboração do Plano, teste e manutenção: A primeira etapa é identificar o funcionamento do negócio. Alevate (2014) traz quatro pilares fundamentais para a construção do plano:

- ➔ Unidade de negócio
- ➔ Processos de negócio
- ➔ Componentes do negócio
- ➔ Ativos

Como parte do plano de continuidade, deve haver simulações de interrupções dos serviços.

O objetivo é organizar e manter o bom funcionamento dos serviços de TI, mesmo que a organização enfrente situações de contingência ou desastre. Fontes (2006) complementa:

> “[...]. Para evitar situações que tragam problemas para a organização, é necessário identificar as ameaças possíveis e monitorar sempre o risco dessa ameaça se concretizar. Dessa forma, com certeza, poderemos ser proativos e minimizar ou evitar várias situações em que a organização ficaria em perigo”.

4 COBIT 4.1

O COBIT (*Control Objectives for Information and Related Technology*) é um guia de boas práticas fortemente focadas em controles, que ajudam a implantação da governança de TI por meio da estruturação de processos de TI alinhados ao negócio de uma organização. O COBIT foi elaborado pelo ISACA (*Information Systems Audit and Control Association*), mantido e distribuído pelo ITGI (*IT Governance Institute*) – Instituto de governança de TI. Sua orientação consiste em objetivos de negócios conectados aos objetivos de TI, provendo métricas e modelos de maturidade.

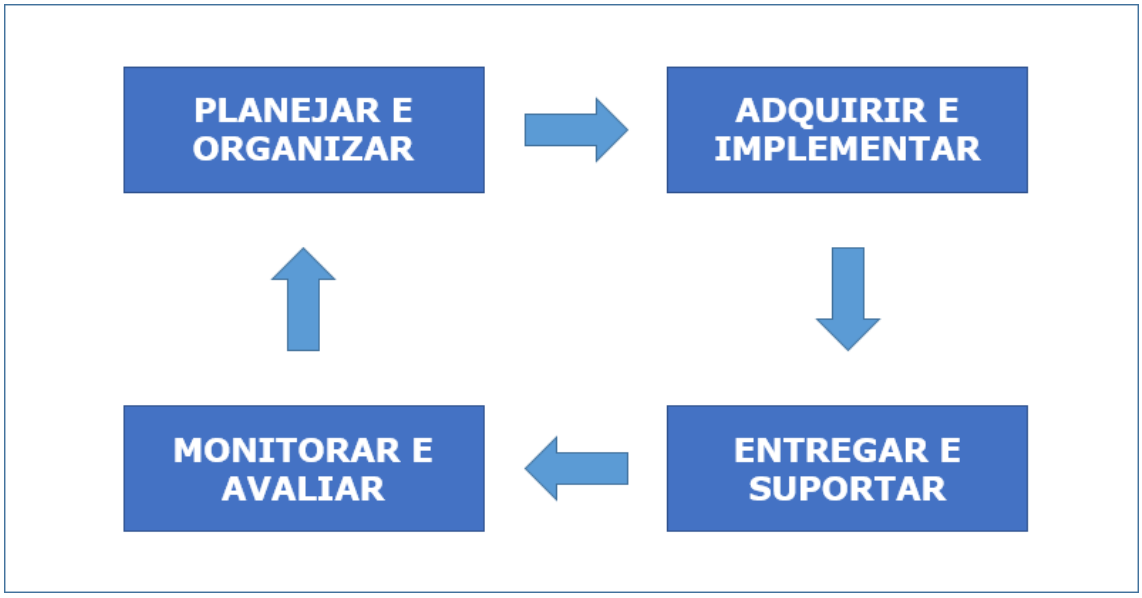
Ferreira e Araújo (2008) apontam o COBIT como um modelo estrutural de controles internos que possibilitam mensurar o desempenho e gerenciar os riscos associados à TI. Seu modelo de gerenciamento é voltado ao nível estratégico, suas estruturas de controles são padronizadas e aceitas mundialmente nos mais variados setores de negócios, principalmente no segmento financeiro.

Manoel (2014) reforça que o COBIT enquadra a segurança da informação dentro da estrutura da governança de TI, orientando a organização a fazer o acompanhamento dos processos, controles e implementação de boas práticas no ambiente tecnológico, de forma segura e auditável.

4.1 ESTRUTURA DO COBIT

COBIT é ilustrado por um modelo que possui trinta e quatro processos divididos em quatro domínios, listados na figura a seguir:

Figura 2 - O *framework* COBIT 4.1.



Fonte: Adaptado de COBIT 4.1 (2007)

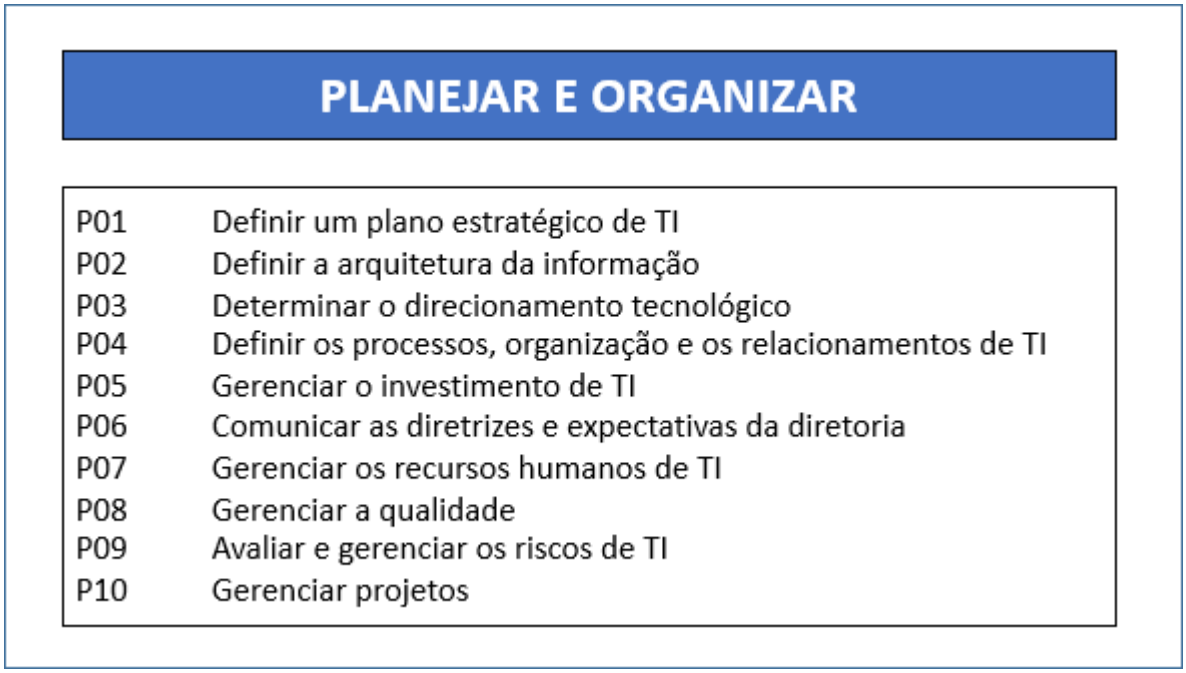
Os quatros domínios constituem de objetivos de controles responsáveis pelo planejamento, aquisição, entrega e monitoração COBIT 4.1 (2007). Ferreira e Araújo (2008) identificam o que são cada um deles:

➔ Planejar e Organizar: Este domínio engloba a parte estratégica e tática, orientada a atingir os objetivos do negócio. Não menos importante, é a maneira como essa estratégia é planejada, comunicada e gerenciada para cada setor dentro da organização.

De forma resumida, esse domínio deve endereçar os seguintes pontos para identificar a melhor forma de atingir os objetivos de TI dentro da organização:

- TI alinhada a estratégia do negócio
- Entendimento e gerenciamento de riscos de TI
- Utilização otimizada de recursos da organização

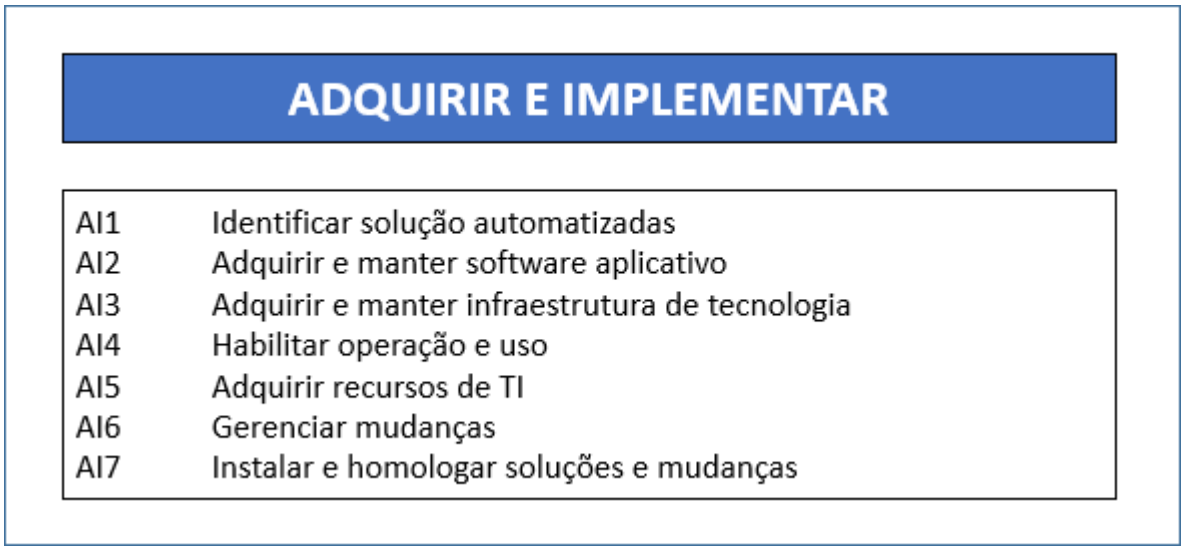
Figura 3 - COBIT: Planejar e organizar



Fonte: Adaptado de COBIT 4.1 (2007)

➔ Adquirir e Implementar: Este domínio lida com mudanças e soluções em um sistema existente, tem como objetivo garantir que continue a atender ao negócio mesmo após implementar uma solução.

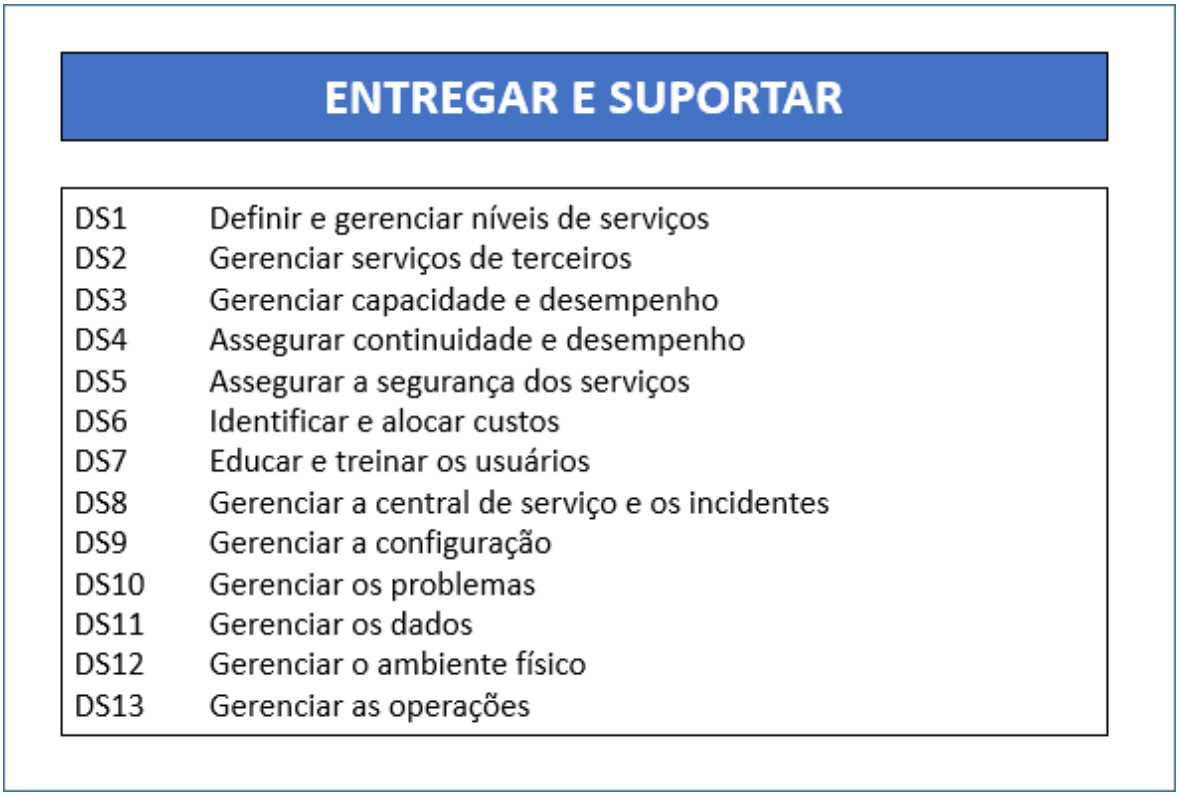
Figura 4 - COBIT: Adquirir e implementar



Fonte: Adaptado de COBIT 4.1 (2007)

➔ Entregar e Suportar: Domínio voltado a entrega de serviços da organização, incluindo a gestão da segurança da informação e continuidade, suporte aos usuários, gerenciamento de dados e instalações. Este domínio contempla o processo foco deste trabalho, o DS4 parte da continuidade de serviços, visto no próximo capítulo.

Figura 5 - COBIT: Entregar e suportar

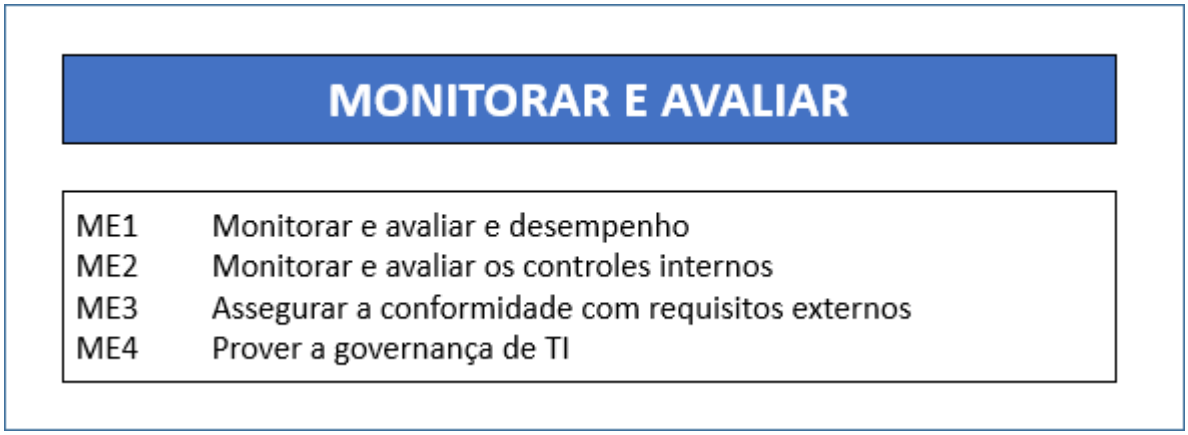


Fonte: Adaptado de COBIT 4.1 (2007)

➔ Monitorar e Avaliar: Voltado a auditoria de qualidade e adequação dos processos de TI, medidos através de indicadores de performance, controles internos e relatórios. São itens pertinentes a este domínio:

- Detecção de problemas proativa;
- Controles internos efetivos e eficientes;
- Medição de riscos, desempenho e conformidade.

Figura 6 - COBIT: Monitorar e avaliar



Fonte: Adaptado de COBIT 4.1 (2007)

4.2 PROCESSO COBIT: DS4 - GARANTIR CONTINUIDADE DOS SERVIÇOS

De acordo com COBIT (2007), a estrutura do processo “DS4 - Assegurar a Continuidade dos Serviços” encontra-se no domínio de entrega e suporte do COBIT 4.1. Este processo foca na disponibilidade dos serviços de TI, através de desenvolvimento, manutenção e testes do plano de continuidade de TI provendo a continuidade dos serviços de TI. São itens indispensáveis deste processo:

- Armazenamento de cópias de segurança;
- Instalações em sítios remotos;
- Treinamentos e testes periódicos do plano de contingência de TI.

O processo ainda é medido por:

- Quantidade de horas perdidas devido à indisponibilidade não planejada;
- Quantidade de processos críticos de negócios, que dependem da TI e não estão cobertos no plano de continuidade de TI da organização.

Se a organização reconhece, realiza e pratica estes passos, ela está garantindo, que se uma interrupção de seus serviços ocorra, o impacto será mínimo.

4.3 MATURIDADE DO PROCESSO

É de suma importância que as organizações tenham conhecimento do estado atual dos processos de seu negócio. Para tal, as organizações devem realizar avaliações para identificar qual sua capacidade em enfrentar situações de interrupções de serviços. Identificando os pontos fortes e fracos em relação a continuidade de negócios. Fontes (2008) utiliza o roteiro dos trinta e quatro processos para definir algumas questões básicas quanto à maturidade:

- Qual o estado atual da organização?
- Qual o estado atual das organizações no mercado?
- Qual estado atual dos padrões de mercado?
- Aonde a organização deseja chegar, e como é planejamento para isso?

O modelo de maturidade é utilizado para medir o desempenho e maturidade do processo de TI, no caso deste trabalho, para avaliar o processo de continuidade dos serviços de TI. Para tal, necessita-se de um gerenciamento do processo de assegurar a continuidade dos serviços de TI, de forma que entregue os serviços com qualidade e atenda às necessidades do negócio, garantindo impacto mínimo na probabilidade de uma interrupção, o modelo de medição escolhido foi o COBIT, onde a maturidade é medida para cada processo.

Através do modelo de maturidade do COBIT, é possível identificar o estágio atual da organização em relação aos concorrentes e o estágio ideal, proposto pelo mercado. Após feita a avaliação e comparação entre a organização analisada, é possível aprimorar os processos onde o medidor encontra-se abaixo do mercado, e determinar um novo objetivo da organização no que se diz ao plano de continuidade de serviços.

No que se refere aos níveis mensuráveis do processo DS4, COBIT (2007) e Fontes (2008) indicam que os níveis são definidos da seguinte forma:

Nível 0 – Inexistente: Quando a organização não possui, ou, desconhece quaisquer processos reconhecidos. Cópias de segurança de dados críticos são inexistentes. Não há atenção devida da direção ao plano de continuidade de serviços.

Nível 1 – Inicial: Quando existem cópias de segurança em um local remoto e gerenciado por um responsável, porém de forma informal e com autoridade limitada ou até mesmo desorganizada, caso uma interrupção ocorra, a reposta da TI seria despreparada, garantindo apenas a continuidade parcial. COBIT (2007) informa que o gerenciamento se encontra em sua forma inicial, levando a organização reconhecer riscos atrelados a continuidade dos serviços, porém não está catalogada como requisito de negócio.

Nível 2 – Repetível: Quando existem recursos de tecnologia alternativos localizados distante do local primário. A organização passou por uma avaliação de impacto dos negócios, levando em consideração seus serviços financeiros, tecnológicos e operacional, determinando uma prioridade de recuperação em caso de desastre. Porém a continuidade de serviços está nos passos iniciais, onde a responsabilidade é estabelecida, no entanto se encontra fragmentada, podendo não ser confiável.

Nível 3 – Definido: Quando a responsabilidade solidária pelo gerenciamento, planejamento e pelos testes da continuidade dos serviços está claramente definida e atribuída. O plano de continuidade de TI é documentado e baseia-se na importância do sistema e no impacto nos negócios. Os testes de continuidade de serviços são realizados, pelo menos duas vezes por ano, mesmo que parcialmente, para garantir a efetividade da solução de recursos alternativos. Os testes são planejados, documentados, avaliados e contam com a participação das áreas usuárias. As pessoas tomam a iniciativa de seguir padrões e recebem treinamento para lidar com a maioria dos incidentes ou desastres. A direção comunica consistentemente a necessidade do plano de assegurar a continuidade de serviço. Componentes de alta disponibilidade e redundância de sistema estão sendo aplicados. É mantido um inventário sobre os componentes e sistemas críticos.

Nível 4 – Gerenciado e Mensurável: Quando existem procedimentos alternativos de recuperação em caso de indisponibilidade dos serviços de TI. Processos devidamente documentados e disponíveis aos usuários, mantidos de forma rigorosa e controlado pela alta gerência. Quanto aos testes, é similar ao nível anterior, devendo ocorrer ao menos duas vezes durante o ano, mesmo que os testes se aplicam à alguns serviços e não ao todo. As equipes envolvidas devem receber treinamento formal e obrigatório. A cada teste é extraído um relatório que apontam

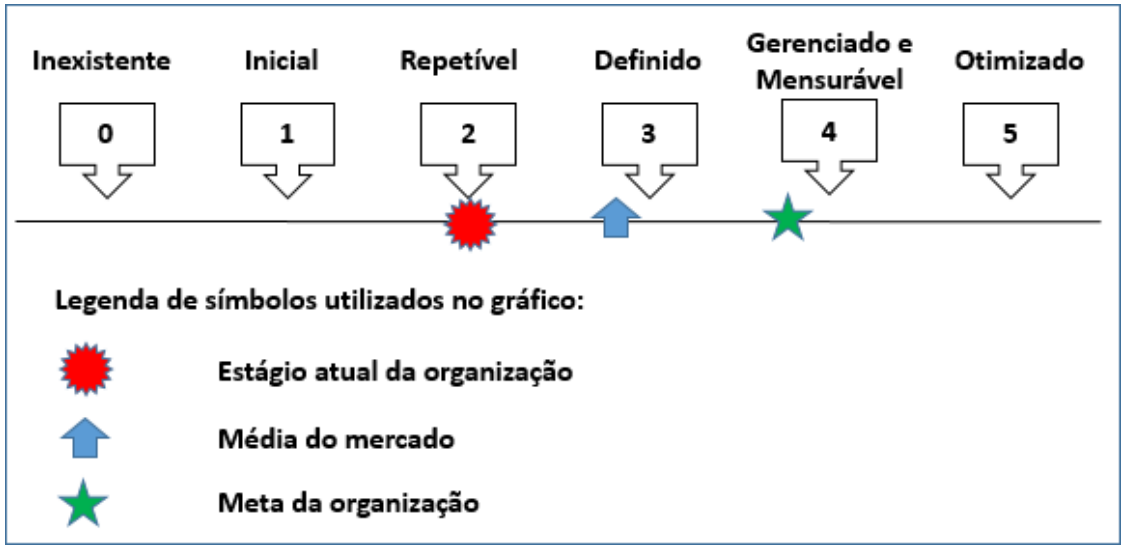
incidentes e riscos a serem classificados e tratados pela TI. Boas práticas de disponibilidade e planejamento são atualizadas de forma constante.

Nível 5 – Otimizado: Quando os responsáveis por procedimentos alternativos de recuperação são definidos e existe uma política de contingência assinada pela alta gerência da organização. Cabe aos responsáveis atualizar e validar o procedimento em vigor, ao menos duas vezes ao ano. Com o resultado obtido nos testes formais, é analisado a necessidade de uma nova atualização ao plano de continuidade.

A organização enxerga a continuidade de serviços considerando a comparação com o mercado através de *benchmarking* e acolhendo as boas práticas.

Cabe à direção integrar a continuidade dos serviços ao plano de continuidade de negócio, assegurando que um desastre ou incidente importante não ocorrerá devido a um único ponto de falha. Toda a organização é notificada a respeito destas práticas de segurança.

Figura 7 - Representação gráfica do modelo de maturidade do COBIT 4.1.



Fonte: Adaptado de COBIT 4.1 (2007)

5 ESTUDO DE CASO: APLICANDO A METODOLOGIA PARA AVALIAR A MATURIDADE DO PROCESSO DS4: ASSEGURAR A CONTINUIDADE DOS SERVIÇOS DE TI

Para o estudo de caso do presente trabalho, buscou-se uma empresa de grande porte no setor financeiro internacional, e por questões de privacidade será tratada neste trabalho com o nome fictício de Banco Sorriso.

O Método utilizado nesta pesquisa foi a utilização de níveis de maturidade de processo obtidos por meio de um questionário para o processo DS4 e seus objetivos de controle, divididos em dez tabelas, onde foi avaliada a maturidade do processo. As questões foram baseadas no modelo de maturidade do COBIT.

Cada objetivo tem o nível avaliado entre zero e cinco, como já apresentado no capítulo anterior, sendo zero o nível inexistente e cinco o nível mais alto da maturidade. Ao final do estudo será somado o nível de maturidade de cada objetivo de processo e feita a média. Desta forma se obtém o resultado final da maturidade do processo.

O questionário foi entregue a um profissional do ramo de tecnologia, responsável pela análise, execuções de testes e documentação do plano de continuidade de serviços da empresa Banco Sorriso. O profissional em questão possui 7 anos de experiência técnica e de gestão em Tecnologia da Informação.

5.1 CENÁRIO ATUAL

A empresa Banco Sorriso possui uma grande estrutura de TI, seu ambiente é constituído de *Mainframes*, servidores *Unix* e *Windows NT* e serviços de rede. Por tratar-se de uma organização financeira, a disponibilidade de serviços é crucial para seu andamento. Toda a infraestrutura física está dividida entre duas localidades, primária e secundária. Entre as localidades primária e a secundária existe uma estrutura que permite o espelhamento das mesmas, em tempo real. Como parte do plano de continuidade da entrega do serviço, a empresa dispõe de funcionários dedicados para manter e atualizar procedimentos e também realizar treinamentos.

Em seu documento oficial de plano de continuidade de negócios está declarado os papéis e as responsabilidades. Cada papel é definido como atividades similares a serem realizadas. No cenário de teste ou desastre real, um indivíduo pode ter mais que um papel, enquanto um papel pode ser desempenhado por mais que um indivíduo.

O time de gerenciamento tático fica responsável por:

- Obter informações sobre o evento, diretamente da pessoa que identificou a situação de indisponibilidade.

- Responder, escalar e documentar internamente os eventos relacionados a interrupção do serviço.

- Orientar todas as ações direcionadas à recuperação.

- Estimar o período de indisponibilidade.

- Garantir que todos os coordenadores técnicos estejam em contato e sintonizados para o início do plano.

- Garantir a todas as pessoas envolvidas no plano, o acesso ao sítio remoto (localidade secundária)

- Determinar o tamanho e proporções dos danos no sítio principal (localidade primária) e juntamente com o time de infraestrutura, definir as ações de reparo.

- Escalar e apresentar reportes detalhados aos Executivos e Coordenadores Técnicos.

Caso algum dos seguintes cenários ocorram, será invocado a continuidade:

- Indisponibilidade de rede, serviços e monitoração;

- Queda de energia e danos a estrutura do edifício.

O plano de contingência contempla suporte para, em caso de um desastre parcial ou completo, os serviços sejam retomados em seu sítio remoto (ou localidade secundária), em um tempo estimado de recuperação de quatro horas.

5.2 APLICAÇÃO DO QUESTIONÁRIO

Para verificar o nível da maturidade do processo de continuidade dos serviços de TI da empresa escolhida, o consultado foi convidado a responder às seguintes questões conforme mostrado nas tabelas a seguir:

Tabela 1 - Questões para avaliar a estrutura de continuidade

Objetivo de controle - DS4.1 – Estrutura de Continuidade	**Nível de Maturidade:**	
Questões para avaliar a maturidade do processo		
Existe um plano de continuidade de negócio para ser seguido caso os serviços de informação fiquem indisponíveis?		
Todas as áreas de negócio foram definidas na gestão da continuidade?		
Existe a identificação de recursos críticos e processos alternativos para sua recuperação?		

Fonte: Próprio autor

Tabela 2 - Questões para avaliar o plano de continuidade de TI

Objetivo de controle - DS4.2 – Planos de Continuidade de TI	**Nível de Maturidade:**	
Questões para avaliar a maturidade do processo		
Existem planos de continuidade de TI voltado à processos fundamentais do negócio em caso de interrupção?		
Existem manuais e procedimentos para a execução de testes?		

Fonte: Próprio autor

Tabela 3 - Questões para avaliar os recursos críticos de TI

Objetivo de controle - DS4.3 – Recursos Críticos de TI	**Nível de Maturidade:**	
Questões para avaliar a maturidade do processo		
Existem prioridades definidas a recursos críticos para o reestabelecimento de serviços de TI?		
Qual o tempo de resposta estimado para a recuperação dos serviços de TI?		

Fonte: Próprio autor

Tabela 4 - Questões para avaliar a manutenção do plano.

Objetivo de controle - DS4.4 – Manutenção do Plano de Continuidade de TI	Nível de Maturidade:	
Questões para avaliar a maturidade do processo		
Existem procedimento e mudanças para assegurar que o plano de continuidade de TI esteja atualizado e refletindo sempre os negócios atuais?		
Como é feita a comunicação com as partes interessadas após mudanças nos procedimentos?		

Fonte: Próprio autor

Tabela 5 - Questões para avaliar o teste do plano.

Objetivo de controle - DS4.5 – Teste do Plano de Continuidade de TI	Nível de Maturidade:	
Questões para avaliar a maturidade do processo		
Qual a frequência de testes realizados para assegurar que os serviços de TI possam ser recuperados de forma efetiva?		
Existem alguma preparação para a realização das atividades de testes de recuperação e documentação dos resultados obtidos durante o exercício?		
Existem implementações de planos de ação de acordo com os resultados obtidos?		

Fonte: Próprio autor

Tabela 6 - Questões para avaliar o treinamento do plano.

Objetivo de controle - DS4.6 – Treinamento do Plano de Continuidade de TI	Nível de Maturidade:	
Questões para avaliar a maturidade do processo		
Existe treinamento com equipes envolvidas no plano de continuidade, de forma regular e baseado na documentação?		
Existe simulação de uma interrupção/desastre, onde os papéis das equipes definidos no procedimento sejam exercidos?		
Qual a frequência de treinamentos de continuidade?		

Fonte: Próprio autor

Tabela 7 - Questões para avaliar a distribuição do plano.

Objetivo de controle - DS4.7 – Distribuição do Plano de Continuidade de TI	**Nível de Maturidade:**	
Questões para avaliar a maturidade do processo		
Como é feita a distribuição do plano de continuidade de TI?		
Existe uma estratégia de distribuição para assegurar que todas as partes recebam o mesmo documento atualizado?		
O plano fica disponível às partes interessadas e autorizadas quando necessário?		

Fonte: Próprio autor

Tabela 8 - Questões para avaliar a recuperação dos serviços de TI.

Objetivo de controle - DS4.8 – Recuperação e Retomada dos Serviços de TI	**Nível de Maturidade:**	
Questões para avaliar a maturidade do processo		
Existem ações a serem executadas nos momentos de recuperação e retomada dos serviços de TI?		
Existem ativações de localizações remotas, incluindo processamento alternativo e comunicação para o cliente e as partes interessadas?		
Existem acordos definindo o tempo de recuperação para assegurar que o negócio retorne à produção?		

Fonte: Próprio autor

Tabela 9 - Questões para avaliar o método de cópias de segurança.

Objetivo de controle - DS4.9 – Armazenamento de Cópias de Segurança em Locais Remotos	**Nível de Maturidade:**	
Questões para avaliar a maturidade do processo		
Existem cópias de segurança e outros recursos críticos de TI armazenadas remotamente?		
O local onde as cópias estão armazenadas é avaliado periodicamente?		
Os dados remotamente armazenados são avaliados quanto à compatibilidade de *hardware* e *software*?		

Fonte: Próprio autor

Tabela 10 - Questões para avaliar a revisão pós retomada dos serviços.

Objetivo de controle - DS4.10 – Revisão Pós-Retomada dos Serviços	Nível de Maturidade:	
Questões para avaliar a maturidade do processo		
Existem procedimentos pós retomada dos serviços de TI?		
Existe alguma ação pós interrupção dos serviços de TI?		

Fonte: Próprio autor

5.3 RESULTADOS

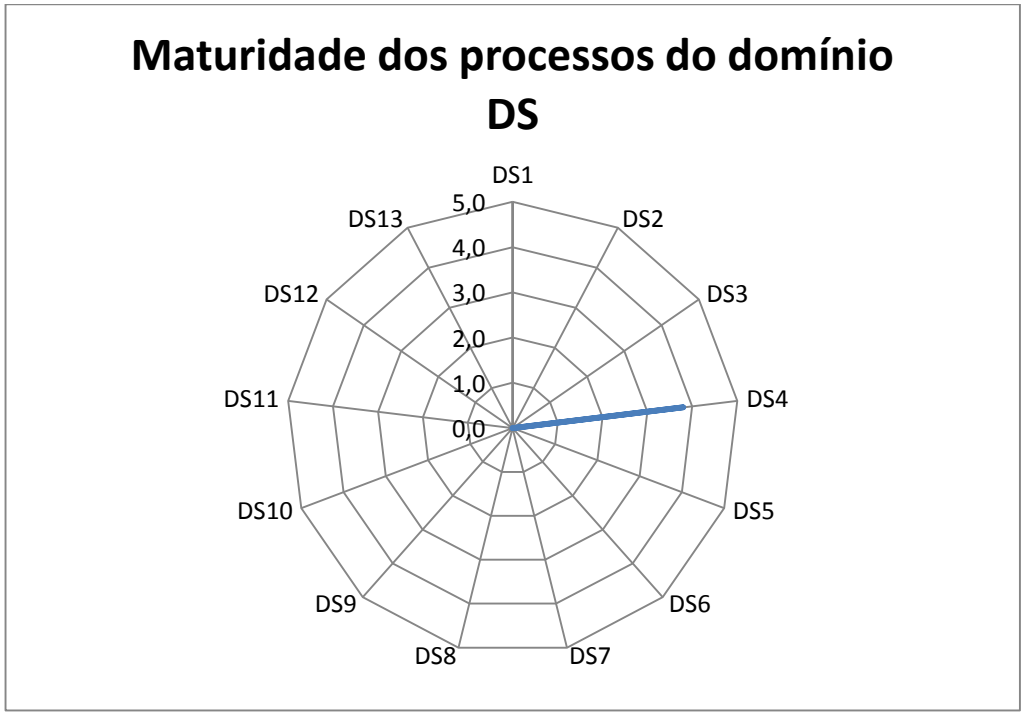
Os resultados obtidos a partir da análise de respostas do profissional entrevistado podem ser observados na tabela a seguir:

Tabela 11 - Resultados da avaliação.

Id		01	02	03	04	05	06	07	08	09	10	Maturidade avaliada
DS - Entregar e Suportar												
DS1	Definir e Gerenciar Níveis de Serviços	0	0	0	0	0	0					0,0
DS2	Gerenciar Serviços Terceirizados	0	0	0	0							0,0
DS3	Gerenciar o Desempenho e a Capacidade	0	0	0	0	0						0,0
DS4	Assegurar a Continuidade dos Serviços	4	3	4	4	3	3	5	4	3	5	3,8
DS5	Garantir a Segurança dos Sistemas	0	0	0	0	0	0	0	0	0	0	0,0
DS6	Identificar e Alocar Custos	0	0	0	0							0,0
DS7	Educar e Treinar os Usuários	0	0	0								0,0
DS8	Gerenciar a Central de Serviço e os Incidentes	0	0	0	0	0						0,0
DS9	Gerenciar a Configuração	0	0	0								0,0
DS10	Gerenciar Problemas	0	0	0	0							0,0
DS11	Gerenciar os Dados	0	0	0	0	0	0					0,0
DS12	Gerenciar o Ambiente Físico	0	0	0	0	0						0,0
DS13	Gerenciar as Operações	0	0	0	0	0						0,0

Fonte: Adaptado de Gaseta (2012)

Figura 8 - Representação gráfica do resultado da maturidade do processo DS4



Fonte: Adaptado de Gaseta (2012)

Seguindo o modelo de maturidade do COBIT 4.1 para o processo DS4 – assegurar a disponibilidade, conclui-se que a empresa do presente estudo de caso possui nível 3.8 de maturidade, tendo alcançado um estado definido do processo, o que caracteriza um nível aceitável de mercado. A empresa apresenta condições de melhorias no processo para poder alcançar os próximos níveis de sua escala de maturidade. Para a empresa alcançar um nível maior de maturidade do processo de disponibilidade, através do modelo COBIT (2007) recomenda-se:

- Investir em recursos necessários que correspondam ao nível 4, mesmo tratando de um processo que possa trazer novos riscos para a organização. Riscos são importantes e devem ser considerados quando saindo de um nível para outro maior de maturidade.

- Incorpore treinamentos com frequência acima do atual plano, realize documentação de cada treinamento, identificando e endereçando as principais falhas de conhecimento técnico do time.

- Manter seu plano alinhado com as melhores práticas externas do mercado.
- Manter o plano de continuidade de TI integrado ao plano de continuidade de negócios, considerando que ambos podem se tornar obsoletos muito rapidamente.
- Garantir o comprometimento contínuo de seus fornecedores e prestadores de serviços.
- Garantir redundâncias, para que uma indisponibilidade ou incidente não ocorra por um único ponto ou falha.
- Utilizar os resultados dos testes formais para fazer os eventuais ajustes necessários e assim manter o plano atualizado.

A documentação deve seguir um padrão de ordem cronológica, exemplificada na tabela 12:

Tabela 12 - Registro de exercícios.

Registro de exercício do plano de continuidade de serviços			
Data do exercício	**Revisões do exercício**	**Responsável (Coordenador)**	**Observações**
Fevereiro 15, 2016			
Maio 20, 2016			
Agosto 15, 2016			
Novembro 10, 2016			

Fonte: Próprio autor

A documentação do registro deve estar atrelada ao plano de execução do teste, armazenada no repositório oficial do processo.

Sugestão de manutenção do planejamento:

- A cada seis meses: Revisão e atualização da lista de softwares e hardwares pelos líderes responsáveis.
- A cada ano: Revisão e alteração dos procedimentos de recuperação.
- A cada ano: Revisão do plano completo pela alta gerência e linha executiva.

6 CONSIDERAÇÕES FINAIS

Este trabalho buscou apresentar conceitos e aspectos que ajudam a implementar a continuidade de serviços em empresas de TI, baseado no guia de boas práticas COBIT.

Constatou-se que através do modelo de maturidade do COBIT foi possível avaliar o nível de maturidade de um processo de controle de uma grande empresa.

Utilizando-se desse método foi possível identificar os pontos mais vulneráveis do processo, onde é possível implementar melhorias e também os pontos fortes que devem ser mantidos de forma a permanecerem atualizados e eficientes.

Para trabalhos futuros, sugere-se utilizar a metodologia COBIT para avaliar outros processos ou até mesmo analisar profundamente um único controle do processo de disponibilidade, a fim de alcançar maiores níveis de maturidade do processo, visando sempre garantir o sucesso contínuo do negócio, mantendo-se competitivo no segmento de mercado.

REFERÊNCIAS BIBLIOGRÁFICAS

ABREU, V.F; FERNANDES A.A. **Implantando a governança de TI**: Da estratégia à gestão de processos e serviços. Rio de Janeiro/RJ: Brasport, 2014.

ALEVATE, William. **Gestão da continuidade de negócios**. Rio de Janeiro: Elsevier Editora, 2014.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS - ABNT. **NBR 10520**: informação e documentação: citações em documentos: apresentação. Rio de Janeiro: ABNT, 2002. 7p.

FERREIRA, Fernando N. F.; ARAÚJO, Márcio Tadeu de. **Política de segurança da informação**: Guia Prático para elaboração e implementação. Rio de Janeiro: Editora Ciência Moderna, 2008. 296 p.

FONTES, Edison Luiz Gonçalves. **Praticando a segurança da informação**: Rio de Janeiro: Editora Brasport, 2008. 283 p.

_____. **Segurança da informação:** o usuário faz a diferença. São Paulo: Editora Saraiva, 2006. 172 p.

GASETA, Edson Roberto. **Fundamentos de governança de TI**. Rio de Janeiro: RNP, 2012.

IT GOVERNANCE INSTITUTE. **COBIT 4.1**. Illinois/USA: IT Governance Institute, 2007.

LYRA, Maurício Rocha. **Segurança e auditoria em sistemas de informação**. Rio de Janeiro: Editora Ciência Moderna, 2008. 253 p.

MAGALHÃES, I.L.; PINHEIRO, W.B. **Gerenciamento de serviços de TI na prática**: uma abordagem com base na ITIL. LOCAL: Novatec, 2007.1000 p.

MANOEL, Sergio da Silva. **Governança de segurança da informação**: como criar oportunidades para o seu negócio. Rio de Janeiro/RJ: Editora Brasport, 2014. 168 p.

MASSIGLIA, Paul; MARCUS, Evan (ed). **The resilient enterprise**: recovering information services from disasters, California/USA: Veritas, 2002. 527 p.

MENEZES, Josué das Chagas. **Gestão da segurança da informação**. Leme/SP. Editora J. H. Mizuno, 2006. 114 p.

SÊMOLA, Marcos. **Gestão da segurança da informação:** uma visão executiva. Rio de Janeiro: Editora Elsevier, 2002. 184 p.

STALLINGS, William; BROWN, Lawrie. **Segurança de computadores**: Princípios e práticas. Rio de Janeiro: Editora Elsevier, 2014. 744 p.